Amendments to the Claims

Claim 1 (previously presented): A method for on-line mass distribution of data products to end users, the method comprising:

maintaining an encrypted first portion of each of said data products at a first location;

maintaining an unencrypted second portion of each of said data products at a second location, wherein said second location is different from said first location;

for each of said end users, confirming the end user's entitlement to one of said data products;

obtaining an unencrypted second portion of said one of said data products on a computing platform from said second location;

after said step of confirming, obtaining an encrypted first portion of said one of said data products on the computing platform from said first location, obtaining a decryption key and using said decryption key to decrypt said encrypted first portion;

combining said decrypted first portion of said one of said data products and said unencrypted second portion of said one of said data products to form a combined product, wherein said step of combining is performed remote from said first location;

storing said combined product on a portable computer-readable storage medium, wherein said combined product is not cryptographically secured on the computer-readable storage medium and said combined product does not include any protection information to limit use of said combined product by the computer platform; and

providing said computer-readable storage medium having said combined first portion and second portion to said user, wherein the first portion of said data product comprises critical data that enables a program executed on the computing platform to use said data product including both the first portion and the second portion together for an intended purpose, wherein said user accesses said combined product from said storage medium with said computer platform at a third location different from said first location and said second location.

Claim 2 (original): The method of claim 1, wherein said data products include geographic databases.

Claim 3 (original): The method of claim 1, wherein said data products include digital copies of movies.

Claim 4 (original): The method of claim 1, wherein said data products include digital copies of musical songs.

Claim 5 (cancelled)

Claim 6 (original): The method of claim 1, further comprising the step of:
prior to the step of combining, encrypting said first portion of one of said data products.

Claim 7 (cancelled)

Claim 8 (previously presented): A system for secure on-line mass distribution of data products to end users comprising:

an authorization server at a first location having associated therewith copies of first portions of a plurality of data products, wherein said first portions of the data products do not include information to enable encrypted data to be decrypted;

a plurality of data distribution terminals at a plurality of locations different from said first location, each of said data distribution terminals has stored thereon copies of second portions of said plurality of data products;

a communications system that provides for exchange of data between said authorization server and said plurality of data distribution terminals,

a data distribution program that provides copies of said data products to those end users who are entitled to have said copies thereof, wherein said data distribution program provides a combined copy of a data product by combining a copy of the first portion of said data product obtained from said authorization server with a copy of the second portion of said data product obtained from one of said plurality of data distribution terminals, wherein said step of combining is performed at a location of said one of said plurality of data distribution terminals and said end user is located at said location of said one of said plurality of data distribution terminals; and a storage device interface associated with said data distribution terminal, wherein said storage device interface stores said combined product on a portable computer-readable storage medium, wherein said combined product is not cryptographically secured on the computer-readable storage medium and said combined product does not include any protection information to limit use of said combined product, wherein said user accesses said combined product from said storage medium with a computer platform at a location different from said location of said data distribution terminal.

Claim 9 (original): The system of claim 8, wherein said authorization server also has associated therewith an authorization database containing data indicating entitlement by said end users to copies of said data products.

Claim 10 (cancelled)

Claim 11 (previously presented): The system of claim 8, wherein the authorization server sends to the data distribution terminal the first portion in encrypted form that can be decrypted using a first decryption key and an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product.

Claim 12 (original): The system of claim 11, wherein the second decryption key is derived as a function of an environmental parameter.

Claim 13 (original): The system of claim 12, wherein the environmental parameter comprises an identification code associated with the entity authorized to access the data product.

Claim 14 (previously presented): The system of claim 11, wherein the data distribution terminal has access to the second decryption key and decrypts the encrypted authorization key, to thereby gain access to the verification information, and to use the verification information to validate use of the data product.

Claim 15 (previously presented): The system of claim 11, wherein the data distribution terminal has access to the second decryption key and decrypts the encrypted authorization information, to thereby gain access to the verification information, and to compare at least a portion of the verification information to predetermined information associated with the user so as to determine whether the user is authorized to access the data product.

Claim 16 (previously presented): The system of claim 15, wherein the predetermined information associated with the user comprises an identification code.

Claim 17 (previously presented): The system of claim 8, wherein the authorization server sends to the data distribution terminal the first portion in encrypted form that can be decrypted using a first decryption key and an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to store the data product.

Claim 18 (original): The system of claim 17, wherein the second decryption key is derived as a function of an environmental parameter.

Claim 19 (original): The system of claim 18, wherein the environmental parameter comprises an identification code associated with the entity authorized to store the data product.

Claim 20 (previously presented): The system of claim 17, wherein the data distribution terminal has access to the second decryption key and decrypts the encrypted authorization key, to thereby gain access to the verification information, and to use the verification information to validate storage of the data product.

Claim 21 (previously presented): The system of claim 17, wherein the data distribution terminal has access to the second decryption key and decrypts the encrypted authorization information, to thereby gain access to the verification information, and to compare at least a portion of the verification information to predetermined information associated with the storage medium so as to determine whether the storage medium is authorized to store the data product.

Claim 22 (original): The system of claim 21, wherein the predetermined information associated with the storage medium comprises an identification code.

Claim 23 (previously presented): The system of claim 8, wherein the data product comprises geographic information.

Claim 24 (canceled)

Claim 25 (previously presented): The method of claim 1, further comprising sending to the second location, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product.

Claim 26 (original): The method of claim 25, further comprising generating the second decryption key as a function of an environmental parameter.

Claim 27 (original): The method of claim 26, wherein the environmental parameter comprises an identification code associated with the entity authorized to access the data product.

Claim 28 (previously presented): The method of claim 27, further comprising:

generating the second decryption key as the function of the identification code;

using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and

using the verification information to validate storage of the data product.

Claim 29 (previously presented): The method of claim 25, further comprising:

using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and

using the verification information to validate use of the data product.

Claim 30 (previously presented): The method of claim 29, wherein using the verification information to validate use of the data product comprises comparing at least a portion of the verification information to predetermined information so as to determine whether the user is authorized to access the data product.

Claim 31 (previously presented): The method of claim 30, wherein the predetermined information comprises an identification code.

Claim 32 (previously presented): The method of claim 1, further comprising sending to the second location, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to store the data product.

Claim 33 (original): The method of claim 32, further comprising generating the second decryption key as a function of an environmental parameter.

Claim 34 (original): The method of claim 33, wherein the environmental parameter comprises an identification code associated with the entity authorized to store the data product.

Claim 35 (previously presented): The method of claim 34, further comprising:

generating the second decryption key as the function of the identification code;

using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and

using the verification information to validate storage of the data product.

Claim 36 (previously presented): The method of claim 32, further comprising:

using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and

using the verification information to validate storage of the data product.

Claim 37 (original): The method of claim 36, wherein using the verification information to validate storage of the data product comprises comparing at least a portion of the verification information to predetermined information associated with the storage medium so as to determine whether the storage medium is authorized to store the data product.

Claim 38 (original): The method of claim 37, wherein the predetermined information associated with the storage medium comprises an identification code.

Claim 39 (previously presented): The method of claim 1, wherein the data product comprises geographic information.